

ON CERTAIN SUBSHIFTS AND THEIR ASSOCIATED MONOIDS

TOSHIHIRO HAMACHI
WOLFGANG KRIEGER

ABSTRACT. Within a subclass of monoids (with zero) a structural characterization is given of those that are associated to topologically transitive subshifts with Property (A).

1. INTRODUCTION

Let Σ be a finite alphabet, and let S_Σ be the shift on the shift space $\Sigma^\mathbb{Z}$,

$$S_\Sigma((x_i)_{i \in \mathbb{Z}}) = (x_{i+1})_{i \in \mathbb{Z}}, \quad (x_i)_{i \in \mathbb{Z}} \in \Sigma^\mathbb{Z}.$$

In symbolic dynamics one studies subshifts, by which are meant the dynamical systems (C, S) , where C is an S_Σ -invariant closed subset of $\Sigma^\mathbb{Z}$, and S is the restriction of S_Σ to C . An introduction to the theory of subshifts is in [Ki, LM] (see also [B, BP]). Here we continue the investigation of the semigroup invariants of subshifts as begun in [Kr]. There a partially ordered set \mathcal{P}_C was invariantly associated to a subshift. Also an invariant property (A) of subshifts was described. If a subshift has Property (A) C then a semigroup (with zero) \mathcal{M}_C is invariantly associated to C . \mathcal{M}_C is a monoid if and only if \mathcal{P}_C is a singleton set and then \mathcal{P}_C contains the unit of \mathcal{M}_C .

Let \mathcal{M} be a semigroup (with zero). We denote by $\Gamma_-(\alpha), \Gamma(\alpha), \Gamma_+(\alpha)$ the left context, context, and right context (in \mathcal{M}) of an element α of \mathcal{M} ,

$$\begin{aligned} \Gamma_-(\alpha) &= \{\gamma_- \in \mathcal{M} : \gamma_- \alpha \neq 0\}, \\ \Gamma(\alpha) &= \{(\gamma_-, \gamma_+) \in \mathcal{M} \times \mathcal{M} : \gamma_- \alpha \gamma_+ \neq 0\}, \\ \Gamma_+(\alpha) &= \{\gamma_+ \in \mathcal{M} : \alpha \gamma_+ \neq 0\}. \end{aligned}$$

Denoting by $[\alpha]$ the set of elements in \mathcal{M} that have the same context as $\alpha \in \mathcal{M}$, the set $[\mathcal{M}] = \{[\alpha] : \alpha \in \mathcal{M}\}$ is a semigroup (with zero), where

$$[\alpha][\beta] = [\alpha\beta], \quad \alpha, \beta \in \mathcal{M}.$$

This product is well defined: for $\alpha, \alpha', \beta, \beta' \in \mathcal{M}$, if $[\alpha] = [\alpha']$, then

$$\begin{aligned} \Gamma(\alpha\beta) &= \{(\gamma_-, \gamma_+) \in \mathcal{M} \times \mathcal{M} : (\gamma_-, \beta\gamma_+) \in \Gamma(\alpha)\} \\ &= \{(\gamma_-, \gamma_+) \in \mathcal{M} \times \mathcal{M} : (\gamma_-, \beta\gamma_+) \in \Gamma(\alpha')\} \\ &= \Gamma(\alpha'\beta), \end{aligned}$$

and if also $[\beta] = [\beta']$, then similarly

$$\Gamma(\alpha' \beta) = \Gamma(\alpha', \beta').$$

We denote by \mathcal{M}^+ (\mathcal{M}^-) the set of elements in $\mathcal{M} \setminus \{0\}$ that cannot be annihilated by multiplication on the right (left).

In section 2 we show that for topologically transitive subshifts C with property (A), the projection of \mathcal{M}_C onto $[\mathcal{M}_C]$ is an isomorphism. We also show that for a topologically transitive subshift C with property (A) and such that

$$\mathcal{M}_C^- \cap \mathcal{M}_C^+ \neq \emptyset,$$

one has that \mathcal{M}_C is a monoid (with zero), and that

$$\mathcal{M}_C^- \cap \mathcal{M}_C^+ = \{\mathbf{1}\}.$$

In the converse direction we consider in section 3 finitely generated monoids \mathcal{M} (with zero) such that

$$\mathcal{M} \setminus \{0\} = \mathcal{M}^+ \mathcal{M}^-,$$

and

$$\mathcal{M}^+ \cap \mathcal{M}^- = \{\mathbf{1}\},$$

and such that every element in \mathcal{M}^+ has a left inverse in \mathcal{M}^- , and every element in \mathcal{M}^- has a right inverse in \mathcal{M}^+ , and such that the projection of \mathcal{M}_C onto $[\mathcal{M}_C]$ is an isomorphism. For a finite generating set Γ of such a monoid \mathcal{M} , we show that the topologically transitive subshift $C(\Gamma) \subset \Gamma^{\mathbb{Z}}$ with admissible words $(\gamma_i)_{1 \leq i \leq I}$ given by

$$\prod_{1 \leq i \leq I} \gamma_i \neq 0,$$

has property (A), and that $\mathcal{M}_{C(\Gamma)}$ is isomorphic to \mathcal{M} .

In section 4 we give examples. These are described in terms of systems of string-rewriting rules.

2. TOPOLOGICALLY TRANSITIVE SUBSHIFTS WITH PROPERTY (A)

We fix notation and terminology. Given a subshift $C \subset \Sigma^{\mathbb{Z}}$, we set for $x \in C$

$$x_{[i,k]} = (x_i)_{i \leq j \leq k},$$

and we set

$$C_{[i,k]} : \{x_{[i,k]} : x \in C\}, \quad i, k \in \mathbb{Z}, i \leq k.$$

We use similar notation also for blocks,

$$b_{[i',k']} = (b_j)_{i' \leq j \leq k'}, \quad b \in C_{[i,k]}, i \leq i' \leq k' \leq k, i, k \in \mathbb{Z}, i \leq k,$$

and also if indices range in semi-infinite intervals. The context of a block $a \in C_{[i,k]}, i, k \in \mathbb{Z}, i \leq k$, is denoted by $\Gamma(a)$,

$$\Gamma(a) = \{(x^-, x^+) \in C_{(-\infty, i)} \times C_{(k, \infty)} : (x^-, a, x^+) \in C\}.$$

With the notation

$$\Gamma^-(a) = \{x^- \in C_{(-\infty, i)} : (x^-, a) \in C_{(-\infty, k)}\}.$$

for the left context of a block we set

$$\omega^+(a) = \bigcup_{n \in \mathbb{N}} \bigcap_{x^- \in \Gamma^-(a)} \{b \in C_{(k, k+n]} : (x^-, a, b) \in C_{(-\infty, k+n]}\},$$

$$a \in C_{[i, k]}, i, k \in \mathbb{Z}, i \leq k.$$

$\omega^-(a)$ has the time symmetric meaning.

In [Kr] a partially ordered set \mathcal{P}_C was invariantly associated to a subshift C . We recall this construction. For a subshift $C \subset \Sigma^{\mathbb{Z}}$ set

$$X_n^+(C) = \bigcap_{i \in \mathbb{Z}} \{x \in C : x_i \in \omega^+(x_{[i-n, i]})\}, \quad n \in \mathbb{N},$$

with the time symmetric meaning for $X_n^-(C)$. We set

$$X_n(C) = X_n^-(C) \cap X_n^+(C), n \in \mathbb{N},$$

Also set

$$X_C^+ = \bigcup_{n \in \mathbb{N}} X_n^+(C).$$

X_C^- has the time symmetric meaning. Also set

$$X_C = \bigcup_{n \in \mathbb{N}} X_n(C).$$

We denote by $P(X_n(C))$ the set of periodic points in $X_n(C)$, $n \in \mathbb{N}$, and also set

$$P(X_C) = \bigcup_{n \in \mathbb{N}} P(X_n(C)).$$

Introduce a reflexive and transitive relation $\leq (C)$ into the set P_C . For $u, u' \in P_C$, $u \geq (C) u'$ will mean that there exists a point in X_C that is negatively asymptotic to the orbit of u and positively asymptotic to the orbit of u' . Denote the resulting equivalence relation by $= (C)$ and the set of $= (C)$ -equivalence classes by \mathcal{P}_C . The partial order that is induced by $\leq (C)$ on \mathcal{P}_C denote also by $\leq (C)$.

In [Kr] the property (A) of subshifts was introduced. For $n, H \in \mathbb{N}$ a subshift $C \subset \Sigma^{\mathbb{Z}}$ is said to have property (a, n, H) , if the following holds: $X_n(C) \neq \emptyset$, and if $i_-, i_+, j_-, j_+ \in \mathbb{Z}$,

$$i_- < i_+ - 3H, \quad j_- < j_+ - 3H,$$

and

$$a \in X_n(C)_{[i_-, i_+]}, \quad b \in X_n(C)_{[j_-, j_+]},$$

$$a_{[i_-, i_- + H]} = b_{[j_-, j_- + H]}, \quad a_{[i_+ - H, i_+]} = b_{[i_+ - H, i_+]},$$

then the context of a is equal to the context of b . A subshift $C \subset \Sigma^{\mathbb{Z}}$ has property (a, n) if there is an $H \in \mathbb{N}$, such that C has property (a, n, H) , and a subshift

$C \subset \Sigma^{\mathbb{Z}}$ has property (A) if there is an $n_o \in \mathbb{N}$ such that for $n \geq n_o$, C has property (A, n).

In [Kr] also a semigroup (with zero) \mathcal{M}_C was invariantly associated to subshifts with property (A). We recall this construction. For a subshift C with Property (A), denote by $Y_n(C)$ the set of points in C that are negatively asymptotic to a point in $P(X_n(C))$ and also positively asymptotic to a point in $P(X_n(C))$, $n \in \mathbb{N}$, and set

$$Y_C = \bigcup_{n \in \mathbb{N}} Y_n(C).$$

One introduces an equivalence relation $\approx (C, H)$ into the set Y_C , where for $u, v \in Y_C$, $u \approx (C) v$ means that for $n \in \mathbb{N}$ such that C has Property (A, n) and such that $u, v \in Y_n(C)$ one has with $q^-, q^+, r^-, r^+ \in P(X_n(C))$ such that u is negatively asymptotic to q^- and positively asymptotic to q^+ , and such that v is negatively asymptotic to r^- and positively asymptotic to r^+ , that

$$q^- = (C)r^-, \quad q^+ = (C)r^+,$$

and with $I^-, I^+ \in \mathbb{Z}$, $I^- < I^+$, $J^-, J^+ \in \mathbb{Z}$, $J^- < J^+$, such that

$$u_{(-\infty, I^-]} = q_{(-\infty, I^-]}^-, \quad u_{[I^+, \infty)} = q_{[I^+, \infty)}^+,$$

$$v_{(-\infty, J^-]} = r_{(-\infty, J^-]}^-, \quad v_{[J^+, \infty)} = r_{[J^+, \infty)}^+,$$

with $H \in \mathbb{N}$ such that C has Property (A, n, H), and with $i^-, i^+ \in \mathbb{Z}$,

$$I^- - i^- > 3H, \quad i^+ - I^+ > 3H,$$

and $j^-, j^+ \in \mathbb{Z}$,

$$J^- - j^- > 3H, \quad j^+ - J^+ > 3H,$$

one has that blocks

$$a \in C_{[i^-, i^+]}, \quad b \in C_{[j^-, j^+]},$$

such that

$$a_{[I^- - H, I^+ + H]} = u_{[I^- - H, I^+ + H]}, \quad b_{[J^- - H, J^+ + H]} = v_{[J^- - H, J^+ + H]},$$

and

$$\begin{aligned} a_{[i^-, I^-]} &\in X_n(C)_{[i^-, I^-]}, & a_{[I^+, i^+]} &\in X_n(C)_{[I^+, i^+]}, \\ b_{[j^-, J^-]} &\in X_n(C)_{[j^-, J^-]}, & b_{[J^+, j^+]} &\in X_n(C)_{[J^+, j^+]}, \end{aligned}$$

and such that

$$a_{[i^-, i^- + H]} = b_{[j^-, j^- + H]}, \quad a_{[i^+ - H, i^+]} = b_{[j^+ - H, j^+]},$$

have the same context.

Let $n, H \in \mathbb{N}$ and let the subshift C have Property (A, n, H). Given $q^+, r^- \in P(X_n(C))$ and $u, v \in Y_n(C)$ such that u is positively asymptotic to q^+ , and v is

negatively asymptotic to r^- we say that a point $x \in Y_C$ is a defining point, more precisely an n -defining point for $[u]_{\approx(C)}[v]_{\approx(C)}$, if there are $I, J \in \mathbb{Z}$, such that

$$u_{[I, \infty)} = q_{[I, \infty)}^+, \quad v_{(-\infty, J]} = r_{(-\infty, J]}^-,$$

and also $I_o, J_o \in \mathbb{Z}, J_o, -I_o > 3H$, such that

$$x_{(-\infty, I_o + H]} = u_{(-\infty, I + H]}, \quad x_{[J_o - H, \infty)} = v_{[J - H, \infty)},$$

and

$$x_{[I_o, J_o]} \in X_n(C)_{[I_o, J_o]}.$$

The construction of the semigroup (with zero) \mathcal{M}_C is completed by defining a binary operation in \mathcal{M}_C by setting for $u, v \in Y_C$, $[u]_{\approx(C)}[v]_{\approx(C)}$ equal to $[x]_{\approx(C)}$, where x is any defining point for $[u]_{\approx(C)}[v]_{\approx(C)}$, whenever such a defining point exists, and by setting $[u]_{\approx(C)}[v]_{\approx(C)}$ equal to zero otherwise. If \mathcal{P}_C is a singleton set, then \mathcal{M}_C is a monoid (with zero) and \mathcal{P}_C contains the unit of \mathcal{M}_C .

(2.1) Lemma. *Let C be a topologically transitive subshift,*

$$X_1(C) \neq \emptyset.$$

Then $Y_1(C)$ is dense in C .

Proof. Let u be a forward and backward transitive point of C , and let $q \in P_1(C)$. Let further $v \in C, K \in \mathbb{N}$. Then there are $J_-, J_+, I \in \mathbb{Z}$, such that

$$J_- \leq I - K, \quad J_+ \geq I + K,$$

and such that

$$u_{I+k} = v_k, \quad -K \leq k \leq K,$$

and

$$u_{J_-} = u_{J_+} = q_0.$$

One defines a point y in C by

$$\begin{aligned} y_i &= q_{i-J_-+I}, & i &\leq J_- - I, \\ y_i &= u_{i+I}, & J_- - I &\leq i \leq J_+ - I, \\ y_i &= q_{i-J_++I}, & J_+ - I &\leq i, \end{aligned}$$

and has then

$$y_i = v_i, \quad -K \leq i \leq K,$$

and

$$y \in Y_1(C). \quad \square$$

(2.2) Lemma. *Let $C \subset \Sigma^{\mathbb{Z}}$ be a subshift with properties $(a, n, H_n), n \in \mathbb{N}$. Let $i_o, j_o \in \mathbb{Z}, j_o - i_o > 3H_1$, let $r \in P_1(C)$ and let $u, v \in Y_1(C)$ be such that*

$$u_{[i_o, \infty)} = r_{[i_o, \infty)}, \quad v_{(-\infty, j_o]} = r_{(-\infty, j_o]},$$

and

$$(1) \quad [u]_{\approx(C)}[v]_{\approx(C)} \neq 0.$$

Then $[u]_{\approx(C)}[v]_{\approx(C)}$ has the 1-defining point

$$(u_{(-\infty, i_o]}, r_{(i_o, j_o)}, v_{[j_o, \infty)}).$$

Proof. Let π be a period of r . By (1) there is an $n \in \mathbb{N}$ such that $[u]_{\approx(C)}[v]_{\approx(C)}$ has an n -defining point, and among the n -defining points of $[u]_{\approx(C)}[v]_{\approx(C)}$ one finds a point $x \in C$ such that there are $I_o, J_o \in \mathbb{Z}, J_o - I_o > 3H_n$, such that

$$x_{(-\infty, I_o + H_n]} = u_{(-\infty, i_o + H_n]}, \quad x_{[J_o - H_n, \infty)} = v_{[j_o - H_n, \infty)},$$

and such that

$$x_{[I_o, J_o]} \in X_n(C)_{[I_o, J_o]}.$$

By Property (a, n, H_n) of C one has for a $J'_o \geq J_o$, such that $J'_o - I_o - j_o$ is a multiple of π , that

$$(u_{(-\infty, i_o]}, r_{(i_o, i_o + J'_o - I_o)}, v_{[j_o, \infty)}).$$

is an n -defining point of $[u]_{\approx(C)}[v]_{\approx(C)}$. Property $(a, 1, H_1)$ of C then implies the lemma \square .

(2.3) Theorem. *Let C be a topologically transitive subshift with property (A). Then the projection of \mathcal{M}_C onto $[\mathcal{M}_C]$ is an isomorphism.*

Proof. To prove the theorem it is enough to consider the situation where one is given $n, H \in \mathbb{N}$ and a subshift $C \subset \Sigma^{\mathbb{Z}}$ with Property (a, n, H) , and $r^-, r^+ \in P(X_n(C))$, together with $v, w \in Y_C$ and $I_0^-, I_0^+, J \in \mathbb{Z}, I_0^+ - H > I_0^- + H, J - H > I_0^- + H$, such that

$$\begin{aligned} v_{(-\infty, I_0^- + H]} &= w_{(-\infty, I_0^- + H]} = r_{(-\infty, I_0^-)}^-, \\ v_{[I_0^- - H, \infty)} &= r_{[I_0^- - H, \infty)}^+, \quad w_{[J - H, \infty)} = r_{[I_0^-, \infty)}^+, \end{aligned}$$

and such that

$$(1) \quad v \not\approx(C) w,$$

and such that the left context of $[v]_{\approx(C)}$ in \mathcal{M}_C is identical to the left context of $[w]_{\approx(C)}$ in \mathcal{M}_C . The task is to show that then the context of $[v]_{\approx(C)}$ in \mathcal{M}_C differs from the context of $[w]_{\approx(C)}$ in \mathcal{M}_C .

By (1) the context of $v_{[I_0^-, I_0^+]}$ differs from the context of $w_{[I_0^-, J]}$. We continue under the assumption that there is a $y \in C$ such that

$$y_{[I_0^-, I_0^+]} = v_{[I_0^-, I_0^+]},$$

and such that

$$(2) \quad (y_{(-\infty, I_0^-)}, y_{(I_0^-, -\infty)}) \notin \Gamma(w_{[I_0^-, J]}).$$

By Lemma (2.1) there are $I_m^-, I_m^+ \in \mathbb{N}$,

$$I_m^- < I_{m-1}^-, I_m^+ > I_{m-1}^+, \quad m \in \mathbb{N},$$

and points $y^{(m)} \in Y_C, m \in \mathbb{N}$, such that

$$(3) \quad y_{(I_m^-, I_m^+)}^{(m)} = y_{(I_m^-, I_m^+)}, \quad m \in \mathbb{N}.$$

Define points $u^{(m, -)}, u^{(m, +)} \in Y_C, m \in \mathbb{N}$, by

$$u^{(m, -)} = (y_{(-\infty, I_0^-]}^{(m)}, r_{(I_0^-, \infty)}^-), \quad u^{(m, +)} = (r_{(-\infty, I_0^+]}^+, y_{[I_0^+, \infty)}^{(m)}).$$

Here

$$[u^{(m, -)}]_{\approx(C)} [v]_{\approx(C)} [u^{(m, +)}]_{\approx(C)} = [y^{(m)}]_{\approx(C)}.$$

It follows that

$$[u^{(m, -)}]_{\approx(C)} [w]_{\approx(C)} \neq 0,$$

and by Lemma (2.2) there is an n -defining point $x^{(m)}$ of $[u^{(m, -)}]_{\approx(C)} [w]_{\approx(C)}$ that is given by

$$(4) \quad x^{(m)} = (r_{(-\infty, I_0^-]}^-, w_{(I_0^-, \infty)}).$$

One sees now that there is an $m_o \in \mathbb{N}$ such that

$$[u^{(m_o, -)}]_{\approx(C)} [w]_{\approx(C)} [u^{(m_o, +)}]_{\approx(C)} = 0.$$

Otherwise it would follow from Lemma (2.2) that there are n -defining points $z^{(m)} \in C, m \in \mathbb{N}$, of $[x^{(m)}]_{\approx(C)} [u^{(m, +)}]_{\approx(C)}$ that are given by

$$(5) \quad z^{(m)} = (x_{(-\infty, J]}^{(m)}, r_{[0, \infty)}^+).$$

By (3), (4) and (5) then

$$\lim_{m \rightarrow \infty} z^{(m)} = (y_{(-\infty, I_0^-)}, w_{[I_0^-, J]}, y_{(I_0^+, \infty)}),$$

which contradicts (3). \square

(2.4) Lemma. *Let C be a topologically transitive subshift with property (A), and let $v \in Y_C$ be such that*

$$[v]_{\approx(C)} \in \mathcal{M}_C^+.$$

then

$$v \in X_C^+.$$

Proof. Consider a topologically transitive subshift $C \subset \Sigma^{\mathbb{Z}}$ with property (a, K) , $K \in \mathbb{Z}_+$. Let $v \in Y_1(C)$,

$$(1) \quad [v]_{\approx(C)} \in \mathcal{M}_C^+,$$

and let $r^-, r^+ \in P_1(X)$ and $i_-, i_+ \in \mathbb{Z}, i_- < i_+$, be such that

$$r_{(-\infty, i_-]}^- = v_{(-\infty, i_-]}, \quad r_{[i_+, \infty)}^+ = v_{[i_+, \infty)}.$$

Set

$$I_o = i_- - 2K.$$

We show that

$$(2) \quad v_{(I_o, \infty)} \in \omega^+(v_{I_o}),$$

which implies that

$$v \in X_{i_+ - I_o}^+(C).$$

To show (2), let

$$u \in C_{(-\infty, I_o]}, \quad u_{I_o} = v_{I_o}.$$

As a consequence of Lemma (2.1) there exist $p^{(n)} \in P_1(C)$, $n \in \mathbb{N}$, and $I_n, I'_n \in \mathbb{Z}$,

$$I'_n < I_n, I_n < I_{n-1}, \quad n \in \mathbb{N},$$

such that one has points $u^{(n)} \in Y_1(C)$ such that

$$u_{(-\infty, I'_n]}^{(n)} = p_{(-\infty, I'_n]}^{(n)}, \quad u_{[I_n, I_o]}^{(n)} = u_{[I_n, I_o]}, \quad u_{[I_o, \infty)}^{(n)} = r_{[I_o, \infty)}^-, \quad n \in \mathbb{N}.$$

From (1)

$$[u^{(n)}]_{\approx C} [v]_{\approx C} \neq 0, \quad n \in \mathbb{N},$$

and by Lemma (2.2) then

$$(u_{(-\infty, I_o]}^{(n)}, v_{(I_o, \infty)}) \in C.$$

It is

$$\lim_{n \rightarrow \infty} (u_{(-\infty, I_o]}^{(n)}, v_{(I_o, \infty)}) = (u, v_{(I_o, \infty)}),$$

and (2) follows. \square

(2.5) Theorem. *Let C be a topologically transitive subshift with property (A) such that*

$$(1) \quad \mathcal{M}_C^- \cap \mathcal{M}_C^+ \neq \emptyset.$$

Then \mathcal{M} is a monoid (with zero), and

$$\mathcal{M}_C^- \cap \mathcal{M}_C^+ = \{\mathbf{1}\}.$$

Proof. We prove that there exists a $p \in P(X_C)$ such that

$$(2) \quad [p]_{\approx(C)} \in \mathcal{M}_C^- \cap \mathcal{M}_C^+.$$

By (1) there is a $y \in Y_C$ such that

$$(3) \quad [y]_{\approx(C)} \in \mathcal{M}_C^- \cap \mathcal{M}_C^+,$$

and by Lemma 2.4

$$(4) \quad y \in X_C.$$

Let p be the periodic point in X_C to which y is left asymptotic, and let q be the periodic point in X_C to which y is right asymptotic. By (2) $[y]_{\approx(C)} \in \mathcal{M}^+$, in particular $[p]_{\approx(C)}[y]_{\approx(C)} \neq 0$, and therefore

$$(5) \quad q \geq (C)p.$$

It follows from (4) and (5) that there is a $\tilde{y} \in [y]_{\approx(C)}$ that is left asymptotic to p and right asymptotic to the orbit of p and such that $\tilde{y} \in X_C$. By Property (A) $[p]_{\approx(C)} = [\tilde{y}]_{\approx(C)}$. It follows from (1) that all periodic points in X_C are (C) -equivalent to p and that $[p]_{\approx(C)} = \mathbf{1}$. \square

3. SUBSHIFTS CONSTRUCTED FROM A CLASS OF MONOIDS

In this section we show for a certain class of finitely generated monoids (with zero) \mathcal{M} and a finite generating set Γ of \mathcal{M} , that the subshift $C(\Gamma)$ has Property (A), and that the monoid (with zero) that is associated to it is isomorphic to \mathcal{M} .

(3.1) Theorem. *Let \mathcal{M} be a finitely generated monoid (with zero) such that*

$$(1) \quad \mathcal{M} \setminus \{0\} = \mathcal{M}^+ \mathcal{M}^-,$$

and such that every element in \mathcal{M}^- has a right inverse in \mathcal{M}^+ and every element in \mathcal{M}^+ has a left inverse in \mathcal{M}^- . Then the following are equivalent:

(a) *There exists a topologically transitive subshift C with property (A) such that \mathcal{M}_C is isomorphic to \mathcal{M} .*

(b) *It is*

$$(2) \quad \mathcal{M}^+ \cap \mathcal{M}^- = \{\mathbf{1}\},$$

and the projection of \mathcal{M} onto $[\mathcal{M}]$ is an isomorphism.

Proof. By Theorems (2.1) and (2.5), (b) is a necessary condition for (a) to hold. Assume (b), and let Γ be a finite generating set of \mathcal{M} . We prove that $\mathcal{P}_{C(\Gamma)}$ has Property (A) and that $\mathcal{M} = \mathcal{M}_{C(\Gamma)}$. The proof is in four parts.

1. Write with $K \in \mathbb{N}$, the unit of \mathcal{M} in terms of the generators in Γ ,

$$(1) \quad \mathbf{1} = \prod_{0 \leq k < K} \gamma_k.$$

and let a periodic point of $C(\Gamma)$ with period K be given by

$$p_k = \gamma_k, \quad 0 \leq k < K.$$

By (1)

$$\Gamma^-(p_{[0,K)}) = C(\Gamma)_{(-\infty,0)},$$

Therefore

$$p_k \in \omega(p_{[0,k)}), \quad 0 < k < K,$$

and also

$$p_K \in \omega^+(p_{K-1}),$$

which shows that $p \in X_K^-(C(\Gamma))$. By a symmetric argument also $p \in X_K^+(C(\Gamma))$. We have shown that $X_{C(\Gamma)}$ is not empty.

2. The hypotheses that every element in \mathcal{M}^- has a right inverse in \mathcal{M}^+ and every element in \mathcal{M}^+ has a left inverse in \mathcal{M}^- , and that the projection of \mathcal{M} onto $[\mathcal{M}]$ is an isomorphism, together with (1) and (2), imply that every element of \mathcal{M} has a unique presentation as a product $\alpha^+\alpha^-$, where $\alpha^+ \in \mathcal{M}^+$, and $\alpha^- \in \mathcal{M}^-$.

To prove that $C(\Gamma)$ has Property (A), let $n \in \mathbb{N}$, let $I_-, I_+ \in \mathbb{Z}$, $I_+ - I_- > 2n$, and let $(\gamma_i)_{I_- \leq i \leq I_+}$ be an admissible word of $C(\Gamma)$ such that

$$(4) \quad (\gamma_i)_{I_-+n \leq i \leq I_+} \in \omega^+((\gamma_i)_{I_- \leq i < I_-+n}), \quad (\gamma_i)_{I_- \leq i \leq I_+-n} \in \omega^-((\gamma_i)_{I_+-n < i \leq I_+}).$$

There are

$$\alpha^+(-), \alpha^+(+) \in \mathcal{M}^+, \quad \alpha^-(-), \alpha^- (+) \in \mathcal{M}^-,$$

given by

$$\prod_{I_- \leq i < I_-+n} \gamma_i = \alpha^+(-)\alpha^-(-), \quad \prod_{I_+-n < i \leq I_+} \gamma_i = \alpha^+(+)\alpha^- (+).$$

Also let $\beta^+ \in \mathcal{M}^+, \beta^- \in \mathcal{M}^-$ such that

$$\alpha^-(-) \left(\prod_{I_-+n \leq i \leq I_+-n} \gamma_i \right) \alpha^+(+) = \beta^+ \beta^-.$$

Here necessarily $\beta^+ = \mathbf{1}$, for otherwise by the hypotheses on the existence of inverses and by (2) there would be $\alpha^-, \eta^- \in \mathcal{M}^-$ such that

$$\alpha^- \alpha^+(-) = \mathbf{1}, \quad \eta^- \beta^+ = 0.$$

With $J, K \in \mathbb{Z}$, $K < J < I_-$, write then α^- and η^- in terms of the generators in Γ ,

$$\alpha^- = \prod_{J \leq i < I_-} \gamma_i, \quad \eta^- = \prod_{K \leq i < J} \gamma_i.$$

Then

$$\prod_{K \leq i \leq I_-+n} \gamma_i \neq 0, \quad \prod_{K \leq i \leq I_+} \gamma_i = 0,$$

which means that the word $(\gamma_i)_{K \leq i \leq I_- + n}$ is admissible for $C(\Gamma)$, but the word $(\gamma_i)_{K \leq i \leq I_+}$ is not, contradicting (4). Symmetrically one has that $\beta^- = \mathbf{1}$. We have shown that

$$\Gamma\left(\prod_{I_- + n \leq i \leq I_+ - n} \gamma_i\right) = \{(\gamma(-), \gamma(+)) \in \mathcal{M} \times \mathcal{M} : \gamma(-)\alpha^+(-)\alpha^- (+)\gamma(+) \neq 0\},$$

and it is seen that the context of the word $(\gamma_i)_{I_- \leq i \leq I_+}$ is determined by the initial and final segments of length n of the word, and this is sufficient to confirm that the subshift $C(\Gamma)$ has Property (A).

3. To show that all periodic points in $X_{C(\Gamma)}$ are $(C(\Gamma))$ -equivalent, let $K \in \mathbb{N}$, and let there be given periodic points $u, v \in X_K(C(\Gamma))$, both with period K . Let $\alpha^-, \beta^- \in \mathcal{M}^-, \alpha^+, \beta^+ \in \mathcal{M}^+$, such that

$$\prod_{0 \leq k < K} u_k = \alpha^+ \alpha^-, \quad \prod_{0 \leq k < K} v_k = \beta^+ \beta^-.$$

By an argument as already seen in the second part of the proof

$$(2) \quad \alpha^- \alpha^+ = \beta^- \beta^+ = \mathbf{1}.$$

Write with $J_0, J \in \mathbb{N}, J > J_0$, α^+ and β^- in terms of the generators in Γ ,

$$\alpha^+ = \prod_{0 \leq j < J_0} \gamma_j, \quad \beta^- = \prod_{J_0 \leq j < J} \gamma_j,$$

and let a point $w \in C(\Gamma)$ be given by

$$\begin{aligned} w_j &= u_j, & j < 0, \\ w_j &= \gamma_j, & 0 \leq j < J, \\ w_j &= v_{J+j}, & j \geq 0. \end{aligned}$$

w is in $X_{C(\Gamma)}$, and we have shown that $u \geq (C(\Gamma))v$, and symmetrically one has that $v \geq (C(\Gamma))u$.

4. Let $y \in Y_{C(\Gamma)}$ be left asymptotic to $q^- \in P(X_{C(\Gamma)})$ and right asymptotic to $q^+ \in P(X_{C(\Gamma)})$. Let $I^-, I^+ \in \mathbb{Z}, I^- < I^+$, such that

$$y_{(-\infty, I^-]} = q_{(-\infty, I^-]}^-, \quad y_{[I^+, \infty)} = q_{[I^+, \infty)}^+,$$

With $\pi(-)$ a period of q^- , and $\pi(+)$ a period of q^+ , let

$$\prod_{I^- - \pi(-) \leq i < I^-} y_i = \alpha^+(-)\alpha^-(-), \quad \prod_{I^+ < i \leq I^+ + \pi(+)} y_i = \alpha^+(+)\alpha^-(+).$$

The mapping that sends $[y]_{\approx(C)}$ to $\alpha^-(-) \prod_{I^- \leq i \leq I^+} y_i \alpha^+(+)$ is an isomorphism of $\mathcal{M}_{C(\Gamma)}$ onto \mathcal{M} . \square

We note that the subshifts $C(\Gamma)$ are coded in the sense of [BH]. Compare here how sofic systems were originally introduced [W]. However, note that no algebraic structure as considered in this section can be finite, since a monoid (with zero) that is associated to a synchronizing system with property (A) is necessarily trivial.

(3.2) Proposition. *Let \mathcal{M} be a monoid (with zero) such that*

$$\mathcal{M} \setminus \{0\} = \mathcal{M}^+ \mathcal{M}^-, \quad \mathcal{M}^+ \cap \mathcal{M}^- = \{1\},$$

and such that every element in \mathcal{M}^+ has a left inverse in \mathcal{M}^- , and every element in \mathcal{M}^- has a right inverse in \mathcal{M}^+ . Let the mappings

$$\alpha_+ \rightarrow \Gamma_-(\alpha_+) \ (\alpha_+ \in \mathcal{M}^+), \alpha_- \rightarrow \Gamma_+(\alpha_-) \ (\alpha_- \in \mathcal{M}^-),$$

be injective. Then the projection of \mathcal{M} onto $[\mathcal{M}]$ is an isomorphism.

Proof. Let $\alpha, \alpha' \in \mathcal{M}$, $\alpha \neq \alpha'$,

$$\alpha = \beta_+ \beta_-, \alpha' = \beta'_+ \beta'_-, \quad \beta_+, \beta'_+ \in \mathcal{M}^+, \beta_-, \beta'_- \in \mathcal{M},$$

and consider the case that

$$\beta_+ \neq \beta'_+,$$

and that there is a $\gamma_- \in \mathcal{M}^-$ such that

$$\gamma_- \in \Gamma_-(\beta_+), \gamma_- \notin \Gamma_-(\beta'_+).$$

Then

$$(\gamma_-, 1) \in \Gamma(\alpha), \quad (\gamma_-, 1) \notin \Gamma(\alpha'). \quad \square$$

4. A CLASS OF EXAMPLES

We describe a class of monoids (with zero) \mathcal{M} such that

$$\mathcal{M} \setminus \{0\} = \mathcal{M}^+ \mathcal{M}^-,$$

such that

$$\mathcal{M}^+ \cap \mathcal{M}^- = \{1\},$$

such that every element of \mathcal{M}^+ has a left inverse in \mathcal{M}^- and every element of \mathcal{M}^- has a right inverse in \mathcal{M}^+ , and such that the mappings

$$\alpha_+ \rightarrow \Gamma_-(\alpha_+) \ (\alpha_+ \in \mathcal{M}^+), \quad \alpha_- \rightarrow \Gamma_+(\alpha_-) \ (\alpha_- \in \mathcal{M}^-),$$

are injective. In these examples \mathcal{M}^+ and \mathcal{M}^- are freely and finitely generated. Let \mathcal{L} be the set of generators of \mathcal{M}^- and let \mathcal{R} be the set of generators of \mathcal{M}^+ . The examples arise by specifying that the generators in \mathcal{L} and \mathcal{R} satisfy relations such that

$$\lambda \rho \in \{0, 1\} \cup \mathcal{L} \cup \mathcal{R}, \quad \lambda \in \mathcal{L}, \rho \in \mathcal{R},$$

and that these relations present the monoid (with zero). Note that these relations determine then the isomorphism type of the monoid (with zero) up to permutations of \mathcal{L} and of \mathcal{R} . These relations also give then rise to a finite confluent monadic system of string-rewriting rules ([BO], for a decision theory see section 4.3). One has for these examples by direct arguments, that if a generator in \mathcal{L} has a right inverse, then it has a word in the generators in \mathcal{R} of length less than or equal to $\text{card}(\mathcal{R})$ as a right inverse. If a generator in \mathcal{L} can be annihilated by multiplication

on the right, then it can be annihilated by a word in the generators in \mathcal{R} of length less than or equal to $\text{card}(\mathcal{R})$. Also, for generators $\lambda, \tilde{\lambda} \in \mathcal{L}, \lambda \neq \tilde{\lambda}$, if their right context differs, then there will be a word in the generators in \mathcal{R} , of length less than or equal to $2\text{card}(\mathcal{L})\text{card}(\mathcal{R})$, that is in the right context of one of them, but not in the right context of the other. A prototype example is here the Dyck inverse monoid (the polycyclic monoid [NP]), that is given by

$$\begin{aligned}\Sigma &= \{\lambda, \lambda', \rho, \rho'\}, \\ \lambda\rho, \lambda'\rho' &\rightarrow \mathbf{1}, \lambda, \rho'\lambda'\rho \rightarrow 0.\end{aligned}$$

Example where $\rho\lambda \in \{0, \mathbf{1}\}, \lambda \in \mathcal{L}, \rho \in \mathcal{R}$ (compare here [Ke]) are

$$\begin{aligned}\Sigma &= \{\lambda, \lambda', \lambda'', \rho, \rho', \rho''\}, \\ \lambda\rho', \lambda\rho, \lambda'\rho', \lambda''\rho'' &\rightarrow \mathbf{1}, \\ \lambda'\rho, \lambda\rho'', \lambda'\rho'', \lambda''\rho, \lambda''\rho' &\rightarrow 0,\end{aligned}$$

and

$$\begin{aligned}\Sigma &= \{\lambda, \lambda', \lambda'', \rho, \rho', \rho''\}, \\ \lambda\rho, \lambda'\rho, \lambda'\rho', \lambda''\rho'' &\rightarrow \mathbf{1}, \\ \lambda\rho', \lambda\rho'', \lambda'\rho'' &\rightarrow 0, \\ \lambda''\rho &\rightarrow 0.\end{aligned}$$

Another example is

$$\begin{aligned}\Sigma &= \{\lambda, \lambda', \lambda'', \rho, \rho', \rho''\}, \\ \lambda\rho, \lambda'\rho', \lambda''\rho'' &\rightarrow \mathbf{1}, \\ \lambda\rho'', \lambda'\rho, \lambda''\rho' &\rightarrow 0. \\ \lambda\rho' &\rightarrow \lambda, \\ \lambda'\rho'' &\rightarrow \lambda', \\ \lambda''\rho' &\rightarrow \lambda''.\end{aligned}$$

REFERENCES

- [B] M.-P. Béal, *Codage Symbolique*, Masson, 1993.
- [BP] M.-P. Béal, D. Perrin, *Symbolic Dynamics and Finite Automata. Handbook of Formal Languages. G.Rozenberg, A.Salomaa, Eds. Vol 2, 463-506*, Springer-Verlag, Berlin, Heidelberg and New York, 1998.
- [BH] F. Blanchard, G. Hansel, *Systèmes codés*, Theoretical Computer Science **44** (1986), 17 - 49.
- [BO] R. V. Book, F. Otto, *String-Rewriting Systems*, Springer-Verlag, Berlin, Heidelberg and New York, 1993.
- [Ke] R. Kemp, *On the average minimal prefix-length of the generalized semi-Dycklanguage*, Informatique théorique et Applications **30** (1996), 545 - 561.
- [Ki] B. P. Kitchens, *Symbolic dynamics*, Springer-Verlag, Berlin, Heidelberg and New York, 1998.
- [Kr] W. Krieger, *On a syntactically defined invariant of symbolic dynamics*, Ergod.Th. and Dynam.Sys. **20** (2000), 501 - 516.

- [LM] D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, Cambridge, 1995.
- [NP] M. Nivat, J.-F. Perrot, *Une généralisation du monoïde bicyclique*, C. R. Acad. Sc. Paris. **271** (1970), 824–827.
- [W2] B. Weiss, *Subshifts of finite type and sofic systems*, Monatshefte Math. **77** (1973), 462 - 474.

Toshihiro Hamachi
Faculty of Mathematics
Kyushu University
744 Motooka, Nishi-ku
Fukuoka 819-0395,
Japan
hamachi@math.kyushu-u.ac.jp

Wolfgang Krieger
Institute for Applied Mathematics
University of Heidelberg
Im Neuenheimer Feold 294
69120 Heidelberg
Germany
krieger@math.uni-heidelberg.de